Session No. 789

In the Path of Disaster – Run, Hide or Prepare?

Sam K. Lee, CSP, CSHM
Chubb Services Corporation
Warren, NJ

Introduction

Corporations can no longer run, hide or ignore the path of disasters. The Swiss Re Sigma report "Number of Events 1970-2005" indicate a steady increase in the number of both "Natural Catastrophes" and "Manmade Disasters" worldwide (see Exhibit 1) since 1970. This trend of rising catastrophes and disasters is indirectly confirmed by the number of Federal Emergency Management Agency (FEMA) declared disasters since 1967 (see Table 1).

Source: Swiss Re, sigma No 2/2006, page 4

Exhibit 1. Number of events from 1970 to 2005

Years	# of FEMA Declared Disasters	Average # of FEMA Declared Disasters
1997 – 2006	**522**	**52.2**
1987 – 1996	**366**	**36.6**
1977 – 1986	**261**	**26.1**
1967 – 1976	**301**	**30.1**

Table 1. Disaster statistics declared by FEMA by decade.

The 2005 hurricane season was the busiest ever recorded with 23 named storms, 11 of which resulted in FEMA-declared disasters. Three of the storms: Katrina, Rita and Wilma were extremely destructive. Katrina insured losses are estimated to be $40 – 50 billion and rising, while Rita and Wilma combined for about $20 billion in insured losses.

In August 2003 there was a massive power outage from Ontario, Canada to the Midwest and MidAtlantic states. Despite the breadth of this disaster, it could have been much worse. Without a quick thinking utility worker in New Jersey who was alert enough to trip a circuit breaker, this power outage would have reached Florida. Weeks would have been added for the country to recover fully from this disaster.

The 9/11 terrorist act had considerable business impact beyond the terrible damage inflicted upon New York City and Washington DC. Interstate commerce came to a halt for several days. All air traffic was suspended for a week. Many financial institutions lost their data centers thus affecting their ability to conduct business for their national and global clients.

These events illustrate that no entity can assume it is immune to a potential disaster. Continued political unrest, aging infrastructure, unpredictable weather patterns, and global warming all have negative trends. Corporate consolidations, centralized processing, overseas vendors and just-in-time management practices are just a few business trends that make companies even more vulnerable.

So if companies cannot run or hide from disasters, then they must prepare for them.

Definitions of a Disaster Recovery Plan

Everyone has their own definition of a Disaster Recovery Plan (DRP) that is neither correct nor wrong. DRP is an encompassing concept that is difficult to grasp. Breaking the DRP into smaller components makes it easier understand. The DRP is composed of four sub plans.

- Avoidance and Preparedness Plan
- Emergency Response Plan
- Business Continuity Plan
- Restoration Plan

Avoidance and Preparedness Plan

Avoidance and Preparedness planning is everything done before a disaster occurs. Companies should include DRP considerations during strategic business planning operations. Companies always consider market accessibility, availability of resources, local operational costs and quality of workforce; but, sometimes forget the DRP issues of expanding an operation. Locating your new operation in a windstorm prone area, flood zone or earthquake zone can be "disastrous." Other proactive actions would include making sure that your fire protection systems are designed for your occupancy and properly maintained, and developing procedures for specific disaster events such as power outages and bomb threats.

Emergency Response Plan (ERP)

Emergency Response planning is everything done immediately after a disaster event occurs. For example, the goal of this plan during a fire is to get everyone out of the building safely and to get the fire event under control. Most companies have excellent ERPs in place because these plans are required by OSHA, industry, state and local regulators.

Business Continuity Plan (BCP)

The Business Continuity Plan addresses the actions needed to be taken immediately after everyone is safe and the disaster event is under control. How do you contact your customers and vendors? How do you continue to deliver your products and services? How do you maintain your revenue stream? Where to resume your operations? These are just a few of the important questions that must be addressed in the BCP. The BCP components are temporary actions taken to keep a company in business until restoration can begin. This is typically the weakest component of a DRP because it is the most difficult to complete. The second half of this paper will focus on BCP planning.

Restoration Plan

The Restoration Plan is designed to bring the business back to the pre-disaster levels. A good plan significantly reduces the time it takes to rebuild the business. Here a few elements of a good Restoration Plan:

- Ensure that adequate funding is available for restoration activities.
- Document procedures for securing building permits or certifying facilities, such as, FDA requirements.
- Identify any building code requirements for new construction. Complete any requirements and secure permits, if possible before the need to build or rebuild.
- Identify critical machinery, software, materials and vendors. Develop and document procedures for quick procurement after a disaster.
- Consider any obstacles (such as, the availability of building materials) that may increase construction time.
- Minimize time to reach operational capacity.

Breaking down DRP into these four components makes it easier to complete and implement. A company can work on components concurrently to save time and improve the final product. Planning teams are less likely to get bogged down in one area and can share information and ideas. When these four component plans are fully integrated, they will result in the best and most functional Disaster Recovery Plan.

Business Continuity Planning

Most companies lack viable Business Continuity Plans (BCP). BC Management's "2005 Benchmark Study Results" indicate that of the 900 companies responding to their survey, only 40% had complete corporate BCPs in place (see Table 2.) leaving 60% of these companies without a viable BCP in place. From my experience, the percentage is even higher because many BCPs in place are out of date, untested and not reliable.

Industry	No BCP Plans	Currently Developing BCP Plans	IT BCP Plans Only	Only Select Departments	Full Corporate-wide BCP Plans	*Total*
Financial/ Banking	0%	6%	3%	29%	62%	34%
Utilities	0%	8%	8%	56%	28%	3%
Healthcare	2%	25%	17%	49%	8%	7%
Insurance	0%	7%	4%	42%	47%	12%
Consulting Services	1%	11%	14%	34%	40%	8%
Manufacturing	6%	8%	17%	47%	22%	4%
Telecommunications	0%	8%	3%	46%	43%	4%
Transportation	0%	17%	25%	50%	8%	1%
Government	2%	16%	10%	43%	29%	7%
Retail	8%	4%	21%	50%	17%	3%
Education	8%	17%	0%	50%	25%	1%
Information/ Data Processing Services	4%	8%	38%	28%	22%	6%
Computer Services/ Systems	6%	12%	24%	35%	24%	4%
Petroleum/ Chemical	0%	20%	0%	80%	0%	1%
Other	2%	11%	15%	50%	22%	5%
*Total**	1%	10%	10%	39%	40%	100%

* This total is a percentage of all survey respondents. For example, 1% of respondents answered "No BCP Plans" for their current Business Continuity program.

Table 2. BC Management's 2005 Benchmark Study Results

BCP planning is an area most companies need to improve upon if they want to enhance the likelihood of surviving a disaster. The BCP details actions needed to make sure a company stays in business immediately after the disaster event is under control and until restoration begins. This plan is initiated after a disaster is formally declared. This plan is critical to ensure an entity's survival after a disaster. The longer it takes to recover, the more revenue and customers they will lose. The longer it takes to recover, the greater the likelihood of a business failure.

There are four basic steps for developing a effective BCP:

- Risk & Business Impact Analysis
- Strategic Planning
- Documentation
- Testing

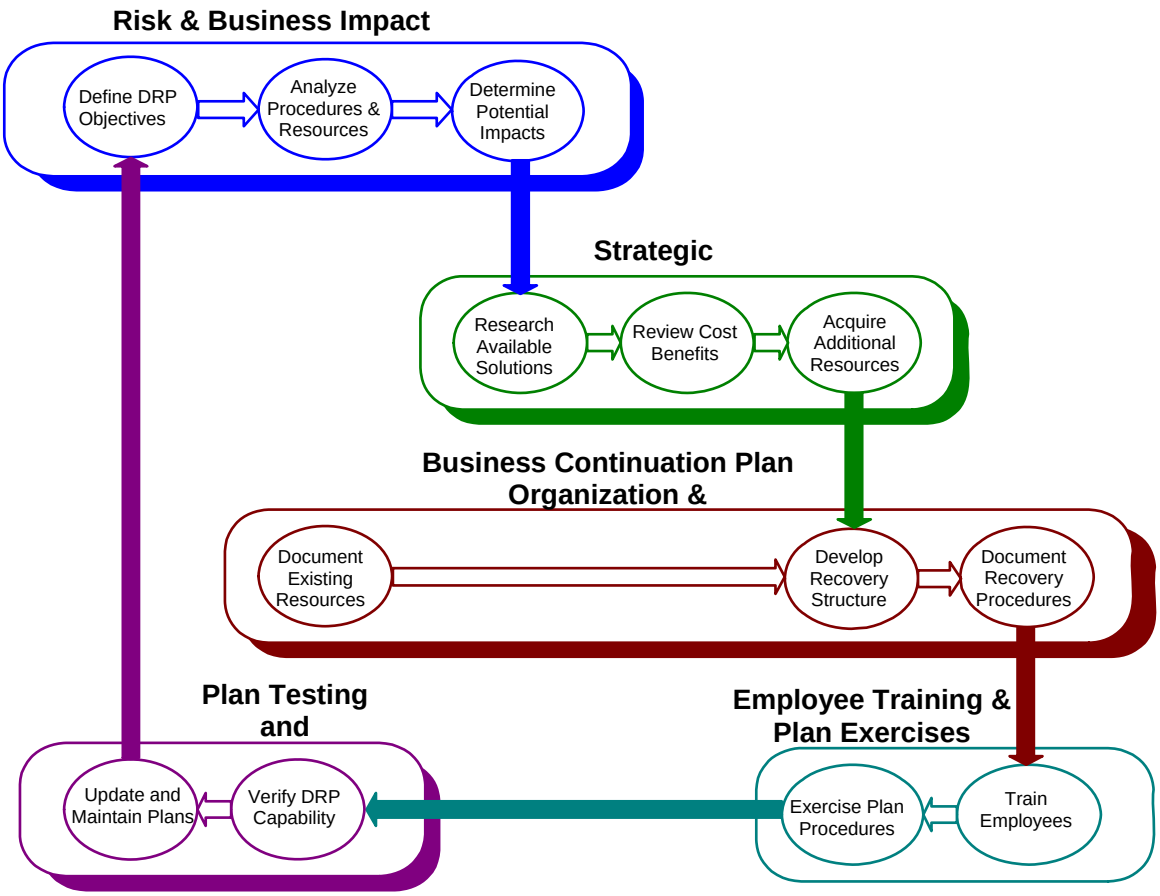

Exhibit 2. Components of a Business Continuity Plan

Risk & Business Impact Analysis

The purpose of the Risk & Business Impact Analysis (R&BIA) is to identify the most critical business processes (CBP), rank them in order of importance and determine the financial impact of each. The R&BIA will uncover operational vulnerabilities and may identify any single points of failure. A single point of failure is the one critical business process that can paralyze an entire company, if it is not recovered quickly. This analysis will define the Return Time Objective (RTO) for each CBP. The RTO is the length of time that a critical business process can be out of service before it severely impacts the company's ability to recover from a disaster. The R&BIA will determine the number of staff needed at remote recovery sites, how quickly they need to recover operations and equipment they will need for their jobs. The findings of the R&BIA must be reviewed and approved by senior management before the BCP project can continue on to the next step – Strategic Planning. The approved R&BIA validates the findings and outlines the financial requirements for developing the Strategic Plan.

Strategic Plan

The purpose of the Strategic Plan is to identify cost effective solutions to the operational vulnerabilities determined in the R&BIA. Strategic Planners use the R&BIA findings, such as

RTOs, and financial impact, to determine a set of solutions for each area of concern. For example, a company may not have a recovery solution for its data center operations. The Strategic Planners may develop a solution table that details recovery capabilities and cost. Senior management uses these solution tables to guide them to in the selection process.

Option	Recovery Time	Capital Costs	Vendor Costs	Annual Costs
Duplicate Facility	**Immediate**	**Very High**	**Low**	**High**
Hot Site Vendor	**3 days**	**Moderate**	**Moderate**	**Moderate**
Quick Ship Equip.	**week**	**Low**	**Low**	**Low**

Table 3. Data Center Disaster Recovery Cost Options

Table 3 demonstrates that the shorter the recovery time, the more expensive the recovery solution. Duplicate data centers are expensive to build and maintain. Setting up a data center at a remote leased facility after a disaster and quickly shipping equipment to it is a low cost solution. A moderate cost recovery option is the use of a commercial hot site to provide a recovery facility and hardware ready for operations. All the company needs to do is bring back up tapes to the hot site to restore their data center operations. Senior management uses the RTO and financial impact data in the R&BIA to help them choose the most cost effective recovery solution. The Strategic Plan report is a compilation of recovery solutions and their respective costs benefits. Before the planners can begin documenting the BCP, senior management must select the recovery solution for each vulnerability.

Documentation

The next phase of the BCP planning process is to document the plan. It should be apparent that documenting a BCP plan without conducting the R&BIA and SP would result in an ineffective plan. Many companies ask for help documenting plans without conducting the first two steps. They should be advised to the impracticality of this request.

The BCP documents the BCP Team Organization and proper protocol for declaring a disaster. This formal declaration initiates the BCP, and is typically made by the Emergency Management Team. The BCP teams report to their designated remote areas and begin to recover the critical business processes assigned to them (see Exhibit 3 “Sample Recovery Solution”). A good BCP should have a modular format for easy access and understanding. The BCP should be customized to meet each specific business objective. An effective BCP is easy to test and maintain.

Testing

Testing is the last phase of the BCP planning process. BCP plans are dynamic in nature and quickly become outdated. Tests validate recovery solutions, train employees and help keep the plan current. BCP testing, training and maintenance apply to all business units, not just management information systems (MIS). BCP testing will uncover areas of weakness and in need of improvement. The testing data and analysis provide important and relevant information for revising and upgrading the BCP. Testing should be conducted semi-annually.

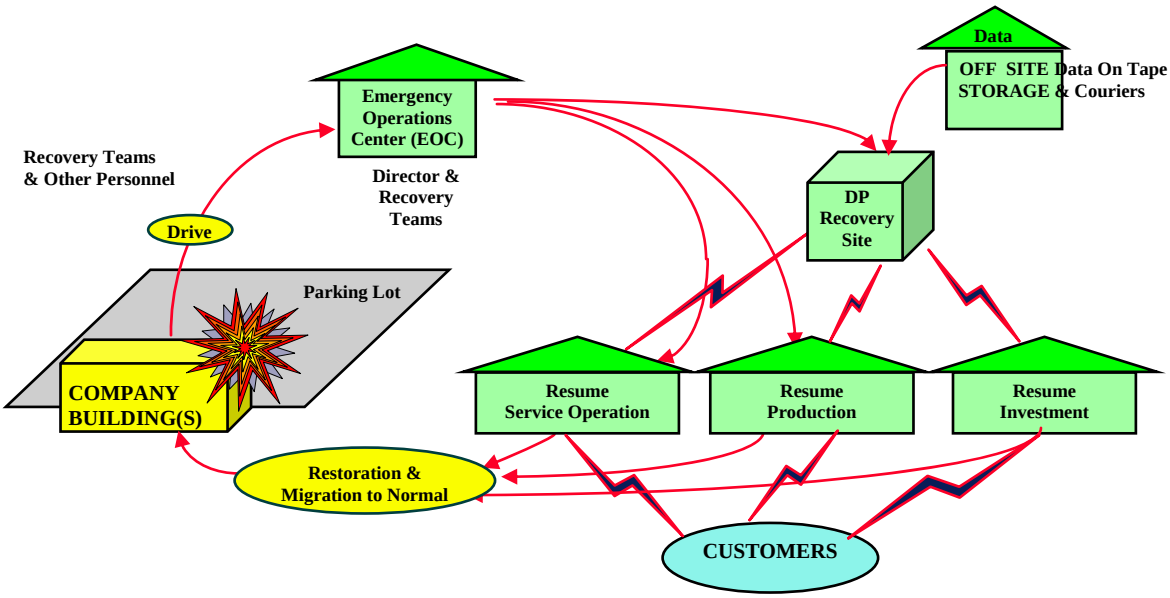

Exhibit 3. Sample recovery solution in action

Conclusion

The sample in Exhibit 3 begins with an incident at the facility. A disaster is declared and the BCP is initiated. BCP teams relocate to their assigned remote locations and begin recovering critical business processes. If the BCP is implemented quickly and precisely, the company should be able to conduct business remotely until normal operations are restored.

Companies cannot run or hide from disasters. If they don't prepare for them, they may go out of business. Businesses who take the time to develop viable Disaster Recovery Plans and test them - **will survive**.